In the Claims

Claims 1, 8, 11, 18, 19, 25, 27, 28, 30 and 32 are currently amended.

Claims 1-33 are pending and are listed below.

1. (Currently Amended) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature;

receiving a security patch;

identifying a vulnerable binary file on a computer based on the binary signature; and

updating the vulnerable binary file on the computer with the security patch.

2. (Original) A processor-readable medium as recited in claim 1, wherein the identifying a vulnerable binary file on a computer includes comparing a bit pattern of the binary signature against binary files located on the computer, the bit pattern associated with a security vulnerability.

3. (Original) A processor-readable medium as recited in claim 1, wherein the updating the vulnerable binary file on the computer includes installing the security patch on the computer.

4. (Original) A processor-readable medium as recited in claim 1, wherein the identifying a vulnerable binary file on a computer includes sending the binary signature to the computer.

5. (Original) A processor-readable medium as recited in claim 4, wherein the updating the vulnerable binary file on the computer includes:

receiving a request from the computer to send the security patch; and

sending the security patch to the computer.

6. (Original) A processor-readable medium as recited in claim 1, wherein the computer is a client computer and the receiving includes receiving the binary signature and the security patch from a distribution server configured to distribute to the client computer, binary signatures that identify vulnerable files and security patches configured to fix the vulnerable files.

7. (Original) A server comprising the processor-readable medium as recited in claim 1.

8. (Currently Amended) A processor-readable medium <u>having a tangible component and</u> comprising processor-executable instructions configured for:

receiving a binary signature that identifies a security vulnerability in a binary file;

receiving a security patch configured to fix the security vulnerability in the binary file; and

distributing the binary signature and the security patch to a plurality of servers.

9. (Original) A processor-readable medium as recited in claim 8, wherein the distributing includes:

sending a notice to each of the plurality of servers regarding the security vulnerability and the available patch;

receiving a request to send the binary signature and the security patch; and

sending the binary signature and the security patch in response to the request.

10. (Original) A distribution server comprising the processor-readable medium as recited in claim 8.

11. (Currently Amended) A processor-readable medium <u>having a tangible component and</u> comprising processor-executable instructions configured for:

receiving a binary signature from a server;

searching for the binary signature in binary files <u>located on a client computer</u>;

sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature;

receiving the security patch from the server; and

updating on the client computer the binary file with the security patch.

12. (Original) A client computer comprising the processor-readable medium as recited in claim 11.

13. (Original) A method comprising:

receiving a binary signature;

searching for a vulnerable file based on the binary signature;

if a vulnerable file is found, requesting a security patch; and

fixing the vulnerable file with the security patch.

14. (Original) A method as recited in claim 13, wherein the requesting includes sending a request to a server for the security patch, the method further comprising receiving the security patch from the server in response to the request.

15. (Original) A method as recited in claim 14, wherein the receiving includes receiving the binary signature from the server.

16. (Original) A method as recited in claim 13, wherein the fixing includes installing the security patch on a computer.

17. (Original) A method as recited in claim 13, wherein the searching includes comparing the binary signature to binary information on a storage medium of a computer.

18. (Currently Amended) A method as recited in claim 17, wherein the binary information is selected from ~~the group~~ a group comprising:

an operating system;

an application program file; and

a data file.

19. (Currently Amended) A method as recited in claim 17, wherein the storage medium is selected from ~~the group~~ a group comprising:

a hard disk;

a magnetic floppy disk;

an optical disk;

a flash memory card;

an electrically erasable programmable read-only memory; and

network-attached storage.

20. (Original) A method comprising:

receiving a binary signature and a security patch from a distribution server;

searching on a client computer for a vulnerable file associated with the binary signature; and

if a vulnerable file is found, fixing the vulnerable file with the security patch.

21. (Original) A method as recited in claim 20, wherein the searching includes transferring the binary signature to the client computer, the client computer configured to search for a vulnerable file associated with the binary signature.

22. (Original) A method as recited in claim 21, wherein the fixing includes:

receiving a request from the client computer to transfer the security patch, the client computer having located a vulnerable file; and

transferring the security patch to the client computer in response to the request.

23. (Original) A computer comprising:

means for receiving a binary signature;

means for searching for a vulnerable file based on the binary signature;

means for requesting a security patch if a vulnerable file is found; and

means for fixing the vulnerable file with the security patch.

24. (Original) A server comprising:

means for receiving a binary signature and a security patch from a distribution server;

means for scanning a client computer for a vulnerable file associated with the binary signature; and

means for fixing the vulnerable file with the security patch if a vulnerable file is found.

25. (Currently Amended) A computer <u>having a tangible component and</u> comprising:

binary information;

a scan module configured to receive a binary signature and scan the binary information for the binary signature; and

a patch module configured to request a security patch and install the security patch if the binary signature is found in the binary information.

26. (Original) A computer as recited in claim 25, further comprising a storage medium configured to retain the binary information.

27. (Currently Amended) A computer as recited in claim 25, wherein the binary information is selected from ~~the group~~ a group comprising:

an operating system;

an application program file; and

a data file.

28. (Currently Amended) A computer having a tangible component and comprising:

binary files;

a binary signature; and

a security patch module configured to receive the binary signature from a server and to scan the binary files in search of the binary signature.

29. (Original) A computer as recited in claim 28, further comprising:

a binary file that includes the binary signature; and

a security patch;

wherein the security patch module is further configured to request the security patch from the server upon locating the binary signature within the binary file, and to apply the security patch to the binary file.

30. (Currently Amended) A distribution server having a tangible component and comprising:

a database; and

a distribution module configured to receive a binary signature and a security patch, store the binary signature and the security patch in the database, and distribute the binary signature and the security patch to a plurality of servers.

31. (Original) A distribution server as recited in claim 30, wherein the distribution module is further configured to receive a request from a server for the binary signature and the security patch and to distribute the binary signature and the security patch to the server in response to the request.

32. (Currently Amended) A server having a tangible component and comprising:

a binary signature associated with a security vulnerability in a binary file;

a security patch configured to fix the security vulnerability in the binary file; and

a scan module configured to scan binary files on a client computer for the binary signature and to update the binary file with the security patch if the binary signature is found.

33. (Original) A server as recited in claim 32, further comprising:

a database;

the scan module further configured to receive the binary signature and the security patch from a distribution server and to store the binary signature and the security patch in the database.